WHAT IS CLAIMED IS:

1. A method for designing an LSI, comprising the step of encrypting provided circuit design data.

2. The method according to claim 1, wherein

the encrypting step includes the step of conducting circuit conversion to produce an encrypted circuit, the circuit conversion being conducted using an entire circuit represented by the circuit design data or a part of the circuit as an original circuit,

the circuit conversion step includes the steps of

providing at least one dummy circuit in parallel with the original circuit, the dummy circuit having a same number of inputs and a same number of outputs as those of the original circuit,

providing a permutation circuit for permutating respective outputs of the original circuit and the dummy circuit, and

providing a selector responsive to a selection signal for selecting a number of signals corresponding to the number of outputs of the original circuit from an output of the permutation circuit so as to produce the encrypted circuit, wherein the selection signal is used as a key signal, and such a value of the key signal that the output of the original circuit matches an output of the selector is used as

a key of the encrypted circuit.

3. The method according to claim 2, wherein

the encrypting step includes the step of producing the dummy circuit to be used in the circuit conversion step, and

the dummy circuit producing step includes the steps of

producing a dummy logic database for the original circuit according to a conversion rule, the dummy logic database including candidate dummy circuits, and

selecting the dummy circuit from the dummy logic database according to an output rule.

4. The method according to claim 3, wherein the conversion rule includes at least one of inversion of a logic value, conversion of a logic operator, and permutation of logic operators.

5. The method according to claim 3, wherein the output rule is random selection.

6. The method according to claim 2, further comprising the step of conducting layout of the encrypted circuit, the layout step including the step of conducting the layout such that an input signal line of the key signal can be connected to either one of a power supply and a ground.

7. The method according to claim 6, wherein the layout step includes the step of connecting the key signal to one of the power supply and the ground according to the key so as to produce layout of the original circuit.

8. A method for verifying an LSI, comprising the step of verifying a circuit operation for circuit design data encrypted together with a reference operation model, the verifying step including the steps of

decoding the encrypted circuit design data into actual design data and the reference operation model,

conducting simulation for the actual design data to obtain an actual output value,

conducting simulation for the reference operation model to obtain an expected output value, and

comparing the actual output value with the expected output value to output a comparison result.

9. A method for verifying an LSI, comprising the step of verifying a circuit operation for circuit design data encrypted together with protocol definition, the verifying step including the steps of

decoding the encrypted circuit design data into actual design data and the protocol definition,

conducting simulation for the actual design data to obtain an actual output value, and

comparing the actual output value with the protocol definition to output a comparison result.

10. A method for verifying an LSI, comprising the step of verifying encrypted circuit design data by simulation, wherein the verifying step limits the simulation conducted by unauthorized access.

11. The method according to claim 10, wherein the verifying step includes the steps of

decoding the encrypted circuit design data into actual design data,

conducting simulation for the actual design data,

counting prescribed limitation information in the simulation, and

limiting the simulation when a count value exceeds an upper limit.

12. The method according to claim 11, wherein the prescribed limitation information includes at least one of an execution step of the simulation, execution time of the simulation, a number of toggles of a specific signal within a circuit, and combination of inputs to the circuit.

13. The method according to claim 12, wherein the prescribed limitation information is randomly selected.

14. The method according to claim 10, wherein the verifying step includes the steps of

decoding the encrypted circuit design data into actual design data,

conducting simulation for the actual design data,

checking in the simulation whether a prescribed protocol restriction condition is violated or not, and

limiting the simulation if the prescribed protocol restriction condition is violated.

15. The method according to claim 14, wherein the prescribed protocol restriction condition includes at least one of an input protocol and an in-operation protocol.

16. The method according to claim 15, wherein the prescribed protocol restriction condition is randomly selected.

17. The method according to claim 11 or 14, wherein the limitation includes at least one of: discontinuing the simulation, reducing a simulation execution speed, and

executing the simulation in an abnormal manner; outputting no simulation result; and producing no data or key to be passed to a following step.

18. A method for verifying an LSI, comprising the steps of:

encrypting circuit design data including a check circuit for checking for unauthorized access in simulation; and

verifying the encrypted circuit design data by simulation, wherein the verifying step operates the check circuit so as to limit the simulation conducted by unauthorized access.

19. The method according to claim 18, wherein the check circuit checks in the simulation whether a count value of prescribed limitation information exceeds an upper limit or not.

20. The method according to claim 18, wherein the check circuit checks in the simulation whether a protocol restriction condition is violated or not.

21. A method for designing an LSI, comprising the steps of:

extracting timing information from provided circuit

design data;

converting the circuit design data into encrypted design data according to a prescribed conversion rule so as to match only the extracted timing information, and adding a buffer to at least one logic gate;

adjusting a size of the added buffer for the encrypted design data; and

by using the prescribed conversion rule as a key, decoding the encrypted design data subjected to the adjustment of the buffer size.

22. A method for designing an LSI, comprising the step of decoding circuit design data encrypted together with a circuit for determining a unique ID into actual design data and the unique-ID determination circuit, the step including the step of defining a correct value in the unique-ID determination circuit by using an input unique parameter.